~~A3~~
B1

processing said telephone call request from the calling card user responsive to said identified user selected options for the calling card.

REMARKS

Claims 1-2, 7-10, 13, 16-17 and 19-20 stand rejected under 35 USC §102(b) as being anticipated by Wallace, U.S. patent 5,988,497. Claims 3-4, 11-12, 14 and 18 stand rejected under 35 USC §103(a) as being unpatentable over Wallace in view of Jankowitz et al., U.S. patent 5,875,236. Claims 5-6 and 15 stand rejected under 35 USC §103(a) as being unpatentable over Wallace in view of Sawyer et al., U.S. patent 6,324,271.

Claims 1, 13 and 20 have been amended to more clearly state the invention. Reconsideration and allowance of each of the claims 1-20, as amended, is respectfully requested.

Wallace, U.S. patent 5,988,497 discloses a dynamic authentication process having multiple tiers of validation. A first tier of validation authenticates the credit transaction based upon static personal identification numbers. If this first tier of validation is satisfied, a threshold determination is made as to whether a secondary tier of validation is required. These thresholds are defined by either the service provider or the card holder to address the additional costs of a second tier of validation. In FIG. 1, the two-tiered validation process begins in step 102 where the system receives a card number from a card holder. Next, in step 104, the system prompts the card holder for a static predefined PIN. In the context of calling cards, the static predefined PIN may exist as a part of the card number itself that is provided to the system. After the static PIN is received, the system determines in step 106 whether the static PIN matches the PIN stored in a database for that account number. If the PINs do not match, the proposed transaction is invalidated in step 108. If one or more thresholds are exceeded (or conditions met) as identified by the determination in step 110, the system then prompts the card holder for a variable PIN in step 112. In various embodiments, the card holder is automatically prompted by a voice response unit (VRU) for computer ordering or calling card use, by an automated teller machine (ATM) for ATM withdrawals, by a computer program when conducting monetary transactions over a computer network (e.g, Internet), etc. In each case, a number can be easily entered on all current authentication devices (e.g., phone key pad, computer key board, etc.) that require input of a transaction amount. If it is determined in step 114 that the variable PINs do not match, the transaction is invalidated in step 116. Alternatively, the card holder could be given additional chances to provide a correct variable PIN. Generally, the invalidation of the transaction in step 116 could also be accompanied by action that labels that particular card as being presumptively fraudulent. This labeling is accomplished through the update of a database record associated with that particular card. After being labeled as presumptively fraudulent, each successive transaction that is based on that card will require the second tier of validation. If the card holder is in the immediate vicinity, the card could also be confiscated. Finally, if the system determines in step 114 that the second tier of validation is satisfied, the transaction is authenticated in step 118. Alternatively, if the system determines in step 110 that the first tier of validation is satisfied and the second tier of validation is not required, the system will also validate the transaction.

Jankowitz et al., U.S. patent 5,875,236 discloses an automated system for detecting and preventing fraudulent telephone calls in a telecommunications network. Prior to completing a telephone call, a database is accessed within a telecommunications network to determine whether the call should be completed. The billing number to which the call is to be charged is compared to a customer record assigned to the billing number and stored in the database. The customer record is checked against a treatment category code which combines geographic call restrictions and thresholding. A call may be identified as potentially fraudulent and blocked if the customer record associated with the billing number indicates that the account is in arrears. In addition, at predetermined intervals during the progress of the call and at the end of each allowed call to be charged to that billing number, the time and/or cost of each call is estimated and added to the total stored in a user-defined threshold counter in the database. When the total stored in the counter exceeds a predetermined threshold limit, a potentially fraudulent call is identified. In this manner, call authorization is performed on a per call basis to prevent fraudulent telephone calls.

Sawyer et al., U.S. patent 6,324,271 discloses a system and method for caller identification, named certified caller ID (CCID) provides an enhancement to existing calling line identification services by providing the terminating end of a telephone call with a cryptographically-certified identity of the caller, rather than the identity associated with the calling telephone line. A less secure variation of CCID could, at the option of the service provider, indicate that the call has been certified if the call were placed using a telephone calling card with a standard PIN. Alternatively, a more secure variation could be implemented in which the authentication took place in conjunction with a known biometric confirmation mechanism such as a fingerprint scanning, voice recognition, iris scanning of the eye, or hand characterization. Since different authentication mechanisms may be used for CCID, it is envisaged that a certification level would be associated with each call and delivered to the terminating end together with the reserved symbol that denotes that the identity of the caller has been certified. The individual or equipment accepting the call could then act on the certification level as appropriate.

Each of the independent claims 1, 13 and 20 has been amended to more specifically define the method, computer program product and system for implementing calling card security of the present invention. As amended, each of the independent claims 1, 13 and 20 recite sequentially checking a plurality of predefined options to identify user selected options for the calling card using a stored calling card record, said calling card record storing a calling card number and a time remaining for the calling card; said calling card record including said plurality of predefined options and each said user selected options for the calling card. This step is not disclosed in the Wallace reference and a combination of all the teachings of the references of record would not achieve the claimed invention as recited by claims 1, 13, and 20, as amended.

The Wallace reference teaches the use of a first tier of validation and a threshold determination made as to whether a secondary tier of validation is required.

These thresholds are defined by either the service provider or the card holder to address the additional costs of a second tier of validation. There is neither an express nor an implied suggestion in the cited Wallace reference for any sequential checking of a plurality of predefined options to identify user selected options for the calling card; nor any suggestion of using a stored calling card record. Only Applicants teach the use of the stored calling card record including said plurality of predefined options and each said user selected options for the calling card. There is neither an express nor an implied suggestion in cited Jankowitz et al. and Sawyer et al. which would have motivated the artisan to modify Wallace reference in a manner which would result in that which is claimed. Consequently, it is submitted that these claims 1, 13 and 20 are patentable.

Dependent claims 2-12 and 14-19 further define the invention of patentable claims 1 and 13, and are likewise patentable.

Applicants have reviewed all the art of record, and respectfully submit that the claimed invention is patentable over all the art of record, including the references not relied upon by the Examiner for the rejection of the pending claims.

It is believed that the present application is now in condition for allowance and allowance of each of the pending claims 1-20 is respectfully requested. Prompt and favorable reconsideration is respectfully requested.

If the Examiner upon considering this amendment should find that a telephone interview would be helpful in expediting allowance of the present application, the Examiner is respectfully urged to call the applicants' attorney at the number listed below.

Respectfully submitted,

By: Joan Pennington
Joan Pennington
Reg. No. 30,885
Telephone: (312) 670-0736

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the Claims:

Please amend claims 1, 13 and 20 as follows:

1. (Amended) A computer implemented method for implementing calling card security comprising the steps of:

receiving a telephone call request from a calling card user;

sequentially checking a plurality of predefined options to identify user selected options for the calling card[;] using a stored calling card record, said calling card record storing a calling card number and a time remaining for the calling card; said calling card record including said plurality of predefined options and each said user selected options for the calling card; and

processing said telephone call request from the calling card user responsive to said identified user selected options for the calling card.

13. (Amended) A computer program product for implementing calling card security with a server computer, said computer program product including a plurality of computer executable instructions stored on a computer readable medium, wherein said instructions, when executed by said server computer, cause the server computer to perform the steps of:

responsive to a user request to setup a calling card, performing setup to receive and store user selected options for said calling card;

receiving a telephone call request from a calling card user;

responsive to said telephone call request from the calling card user, sequentially checking a plurality of predefined options to identify user selected options for the calling card[;] using a stored calling card record, said calling card record storing a calling card number and a time remaining for the calling card; said calling card record including said plurality of predefined options and each said user selected options for the calling card; and

processing said telephone call request from the calling card user responsive to said identified user selected options for the calling card.

20. (Amended) A system for implementing calling card security comprising:

a server computer;

a calling card security program including a plurality of computer executable instructions stored on a computer readable medium, wherein said instructions, when executed by said server computer, cause the server computer to perform the steps of:

receiving a telephone call request from a calling card user;

sequentially checking a plurality of predefined options to identify user selected options for the calling card[;] using a stored calling card record, said calling card record storing a calling card number and a time remaining for the calling card; said calling card record including said plurality of predefined options and each said user selected options for the calling card; and

processing said telephone call request from the calling card user responsive to said identified user selected options for the calling card.